

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

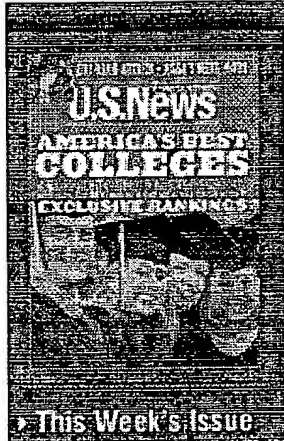
Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

bullish performance.
bearish price.



Rankings & Guides

Money & Business

Education

Health

Columnists

Technology

Best of the Web

Life Online

Gadgets

Privacy

Washington Whispers

Work & Career

News

Briefings

Past Issues

News Quiz

Photography

U.S. News Store

Customer

High-tech card fraud goes on right behind your back

By Margaret Mannix

Do you know where your credit card is? Safely tucked inside your wallet, you say. But how safe is your account, never mind the card? These days, a credit card *number* is a valuable commodity to thieves. "You don't need the plastic to use somebody's credit card number," particularly in this era of Internet and catalog shopping, says Beth Givens, director of the Privacy Rights Clearinghouse in San Diego. The same applies to debit cards. A thief armed with a debit card number can go on a shopping spree, financed by your checking account.

Tech-savvy criminals are devising new ways to get their hands on card information. They've figured out that card fraud beats holding up someone at gunpoint. Instead, they're hacking into Internet databases filled with customer card data and copying account details encoded on a card's magnetic stripe. "Credit card fraud is the bank robbery of the future," says Gregory Regan, special agent in charge of the financial crimes division of the U.S. Secret Service. "[Criminals] have realized that credit cards and the banking system are easy pickings."

Not surprisingly, the Internet is fueling such fraud.

DRE

email



E



fi

also

Acce
usne
full o
priva

Service

About U.S.

News

Advertise

Market@usnews

Sponsored Links

Peace Corps
Redefine Your World
Service, dedication,
idealism.
www.peacecorps.gov

**Habitat for
Humanity**
Donate your car to
Habitat or other
charities. Tax
deduct.
www.donationline.com

Donate to Charity
100% Tax-
Deductible
Donations Free
Pickup. No Hassles!
www.giftsforsight.org

It not only helps criminals retrieve account data quickly and efficiently, but it allows them to perpetrate scams from anywhere in the world. Thieves can E-mail account information overseas to cohorts, who then produce counterfeit cards. Or items can be purchased from an Internet merchant, allowing the fraudster to cloak his identity and leave few clues to track him down. "Any time you are in a non-face-to-face environment, it always makes it easier for fraud," says Rich Detura, director of fraud policy for Citibank.

Easy prey. The astounding growth in electronic-commerce sites provides criminals with a world of merchants to patronize for products that are easily fenced. "No matter how somebody might get ahold of a consumer's financial information, the ability to abuse it on the Internet is huge," says Susan Grant, director of the National Fraud Information Center in Washington. ←

According to the U.S. Secret Service, the fastest-growing ploy used by criminals—particularly organized groups overseas—is to nab card data by "skimming" them off a genuine card. The magnetic stripe on the card's back is encoded with a cardholder's name, account number, expiration date—and a code unique to each piece of plastic. Without the last number, the card cannot be counterfeited. But thieves are buying magnetic stripe readers—available for about \$400 on the Internet—and altering them to record *all* of the data on a magnetic stripe with a mere swipe of the card.

Last November, for example, a Bloomingdale's shopper in New York paying for sunglasses with a credit card noticed something fishy. The card was swiped twice, once through the store's credit card device and also through a store vendor's Palm organizer, which had a skimming device attached

to it. Law enforcement authorities often see this ploy at restaurants, where a dishonest waiter or waitress will unobtrusively pull the small device out of his or her pocket, swipe the card, and hide it before anyone's the wiser.

Some criminals set their sights higher. Recently, a computer hacker obtained thousands of credit card numbers of CD Universe Web site customers and published them on the Internet after the company refused to pay a ransom. "CD Universe basically left the storefront open," says Raf Sorrentino, vice president of fraud and risk management at First Data Corp., an electronic payment processor in Atlanta. The company says security is important, and "obviously it will be even more paramount now," says Brett Brewer, vice president of electronic commerce for eUniverse, which owns CD Universe. Yet experts contend that the firms are partly to blame. "We have companies rushing online trying to cash in on this E-commerce craze and not paying enough attention to security," says Elias Levy, chief technology officer of SecurityFocus.com, a Web information security firm in San Mateo, Calif.

Numbers game. A less sophisticated method of filching card numbers is the many software programs, found free on the Web, that generate numbers using the same algorithms as those used by banks. Anyone with modest computer skills can produce up to 999 card numbers from one card, says Mark Batts, supervisory special agent with the FBI's financial institutions fraud unit. Early last year, the Federal Trade Commission charged several individuals and businesses with illegally billing 783,947 credit and debit card accounts for Internet services. How did the companies get the information? From a bank, which sold them the numbers.

Of course, thieves still acquire credit card

numbers the old-fashioned way, such as dumpster diving and stealing mail. Federal law caps credit card liability at \$50 in fraudulent charges. With a credit card, it's not your money at risk. But if someone uses your debit card number, the funds in your checking, savings, or brokerage account—whatever the number is tied to—can be drained. And your line of credit is up for grabs, too. Meanwhile, checks bounce and insufficient-funds fees pile up, and you're left to sort out the damage.

Such a predicament can exact an emotional toll. Leitha Foote's bank didn't quibble when someone withdrew \$192 last month from the Dallas woman's checking account using her debit card number. It returned the money immediately, pending an investigation, and canceled the card. "I have no idea how anybody else got the card number," says Foote. "I feel very violated." Consequently, Foote now questions the wisdom of a debit card, which she had liked using to easily pay recurring monthly bills. "This has made me really second-guess whether I am going to continue that convenient lifestyle," says Foote.

Preventing scammers from getting their mitts on your card number is a lot tougher than safeguarding the plastic. "There is not a whole lot the consumer can do," says Wesley Wilhelm, director of consulting for eHNC, a subsidiary of HNC Software, a fraud detection and prevention provider in San Diego. Still, consumers should be cautious about disclosing their card number—never giving it to a caller claiming to be, say, your banker, or to a Web site that appears lax in its security. And try to watch your card whenever it's being swiped.

Fraud alarm. Most important, review your account statements carefully, and notify your bank immediately of any discrepancies. "Look at that

statement the minute it comes," says Linda Sherry, editorial director of Consumer Action in San Francisco. Jim Smith of Milwaukee learned that the hard way. He failed to spot three withdrawals of \$19.95 from his checking account via his debit card number in 1998. He finally discovered them when a fourth withdrawal was made last year, causing a check to bounce. While his bank reimbursed him for the latest withdrawal, it refused to compensate him for the earlier ones, saying he had waited too long to notify the bank. "I pay closer attention to my statements now," says Smith. "I go every week and do a balance check on my account at the ATM to make sure everything is OK." (After *U.S. News* called Smith's bank in reporting this story, it agreed to reimburse him for the earlier withdrawals.)


Though the credit card industry empathizes with victims, it says it has been getting a handle on fraud. While skimming has increased in recent years, "the growth has not been what we consider explosive," says John Shaughnessy, senior vice president of risk management for Visa U.S.A. Neural network systems, which can pick up suspicious cardholder usage patterns, and other high-tech measures are helping the issuers combat fraud.

Still, no detection system is foolproof, and the industry has several new fixes on the drawing board. Visa and MasterCard have introduced another validation code, printed on the back of the card, which merchants who accept "card not present" transactions can request of cardholders. Other solutions include technology that will read the properties of the magnetic stripe.

The associations are also working with merchants to help detect fraud in phone and Internet transactions. After all, it's the retailer who gets stuck with the fake transaction. "Typically, the

merchant ends up eating that," says Robert McKinley, president of CardWeb, a Gettysburg, Pa., firm that researches credit cards. Meanwhile, the industry is pushing for widespread adoption of a secure electronic transaction protocol which would create a digital ID for cardholders and merchants. Issuers are weighing in, too. Citibank cardholders, for example, can sign up for "ClickCredit," a separate line of credit and account number to be used exclusively for online buys. Other firms are creating secure payment methods, such as virtual "wallets" for Web purchases.

In the future, many worry that more card fraudsters will go a step further. Identity theft is a huge problem, and a clever con artist can use account information to establish a parallel identity. Victims of fraud are quickly learning the trade-offs of whiz-bang technology. "Privacy is a rare bird these days and becoming much more rare every time we invite someone to access our personal information for the sake of convenience," says Foote. It's a lesson all cardholders should heed.

 [Back to Top](#)

bullish performance.
bearish price.



Copyright © 2003 U.S. News & World Report, L.P. All rights reserved.
Use of this Web site constitutes acceptance of our Terms and Conditions
Privacy Policy.

[Subscribe](#) | [Text Index](#) | [Terms & Conditions](#) | [Privacy Policy](#) | [Contact Us](#)
[Advertise](#)